



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Roger R. DUBE

Application No: 10/003,572

Filed: October 30, 2001

For: ELECTRONIC FILE PROTECTION USING
LOCATION

Docket No: DATIP002

Group Art Unit: 2136

Examiner: Ronald Baum

Date: July 21, 2006

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 21, 2006.

Signed: _____

Joe A. Brock

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION -- 37 CFR 41.37)

Mail Stop Appeal Brief-Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

This Appeal Brief is in furtherance of the Notice of Appeal filed in this case on March 17, 2006, and received in the United States Patent & Trademark Office on March 21, 2006. As the Notice of Appeal was received at the United States Patent & Trademark Office on March 21, 2006, a two month extension of time is hereby requested.

This application is on behalf of:

☒ Small Entity ☐ Large Entity

Pursuant to 37 CFR 41.20(b)(2), the fee for filing the Appeal Brief is:

☒ \$250.00 (Small Entity) ☐ \$500.00 (Large Entity)

07/25/2006 MBELETE1 00000037 10003572

02 FC:2252

225.00 0P

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136 apply:

☒ Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

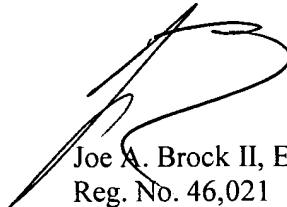
<u>Months</u>	<u>Large Entity</u>	<u>Small Entity</u>
<input type="checkbox"/> one	\$120.00	\$60.00
<input checked="" type="checkbox"/> two	\$450.00	\$225.00
<input type="checkbox"/> three	\$1020.00	\$510.00
<input type="checkbox"/> four	\$1,590.00	\$795.00

Total Fees Due:

Appeal Brief Fee	\$ <u>250.00</u>
Extension Fee	\$ <u>225.00</u>
Total Fee Due	\$ <u>475.00</u>

☒ Enclosed is PTO-2038 Credit Card Payment Form for the amount of \$475.00.

Respectfully submitted,
PATENT VENTURE GROUP
A PROFESSIONAL LAW CORPORATION



Joe A. Brock II, Esq.
Reg. No. 46,021

10788 Civic Center Drive, Suite 215
Rancho Cucamonga, CA 91730
(909) 758-5145
Customer No. 52758



PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**In re Application of:
Roger R. DUBE**

Application for Patent

Filed October 30, 2001

Application No. 10/003,572

FOR:

ELECTRONIC FILE PROTECTION USING LOCATION

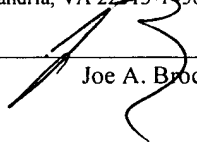
APPEAL BRIEF

**Group Art Unit: 2136
Examiner: Ronald Baum**

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA ~~22313~~ 22314-1450 on July 21, 2006.

Signed: _____


Joe A. Brock

07/25/2006 MBELETE1 00000037 10003572

01 FC:2402

250.00 0P

**PATENT VENTURE GROUP
A PROFESSIONAL LAW CORPORATION
Attorneys for Applicant**



TABLE OF CONTENTS

	<u>Page No.</u>
I. REAL PARTY IN INTEREST	1
II. RELATED APPEALS AND INTERFERENCES	1
III. STATUS OF CLAIMS	1
IV. STATUS OF AMENDMENTS	1
V. SUMMARY OF THE CLAIMED SUBJECT MATTER	1
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	4
VII. ARGUMENTS	4
ISSUE 1 - WHETHER CLAIMS 1-6, 15-22, 26, AND 28-29 ARE PATENTABLE UNDER 35 USC 102 OVER <u>FISCHER '617?</u>	4
<u>Claims 1-6</u>	4
<u>Claims 15-22</u>	7
<u>Claims 26, 28-29</u>	9
ISSUE 2 - WHETHER CLAIMS 7-9 AND 23 ARE PATENTABLE UNDER 35 USC 103 OVER <u>FISCHER</u> IN VIEW OF <u>OVERFIELD '577?</u>	10
<u>Claims 7-9 and 23</u>	10
ISSUE 3 - WHETHER CLAIMS 10-14 AND 24-25 ARE PATENTABLE UNDER 35 USC 103 OVER <u>FISCHER</u> IN VIEW OF <u>SCHNECK ET AL '498?</u>	10
<u>Claims 10-14 and 24-25</u>	10
APPENDIX A - CLAIMS ON APPEAL	
APPENDIX B - EVIDENCE	
APPENDIX C – RELATED PROCEEDINGS	



I. REAL PARTY IN INTEREST

The real party in interest is Digital Authentication Technologies, Inc., the assignee of the present invention.

5 II. RELATED APPEALS AND INTERFERENCES

Co-pending appeal for commonly owned U.S. Application No. 09/948,730, filed September 7, 2001, by inventor Roger R. Dube, and entitled "METHOD AND APPARATUS FOR REAL-TIME DIGITAL CERTIFICATION OF ELECTRONIC FILES AND TRANSACTIONS USING ENTROPY FACTORS."

10

III. STATUS OF CLAIMS

Claims 1-26 and 28-29 are pending in the subject application. Claims 27, 30-38 have been cancelled. Claims 1-26 and 28-29 have been finally rejected and are on appeal.

15 IV. STATUS OF AMENDMENTS

The Applicant has not submitted any amendment subsequent to final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

To protect electronic files on a computer, all the embodiments of the present invention recite a value termed a "delay number," which is a measure of the variation between the arrival times of two timing signals received from a *single* remote source, such as a satellite (see, e.g., page 16, lines 12-14, page 17, lines 3-15, and page 25, lines 4-18 of the instant specification). Variations in the ionosphere and atmosphere due to weather, barometric pressure, solar activity, and other variable and unpredictable parameters generally cause the purity of the timing signals to fluctuate, causing unpredictable delays in the timing signals. Embodiments of the present invention use a measure of these variations, called a delay number, as an unpredictable random number for use in protecting electronic files. Advantageously, the delay number depends on the moment to moment value of the various parameters along the path from the satellite to the receiver. Therefore, the delay is specific to each satellite and receiver at a specific time and a specific location, and is extremely difficult, if not impossible, to calculate remotely, thus preventing

hacking, breaking, deciphering, or otherwise “spoofing” the system. The following embodiments are based on a computer in communication with a receiver capable of receiving signals from a remote source. (See, e.g., page 17 lines 3-15 of the instant specification for detailed description of the delay number usage).

5 A first embodiment of the subject invention is exemplified in claim 1 which recites a method for protecting electronic files on a computer. The method includes receiving first and second timing signals 404a and 404b from a remote source, such as a Global Positioning Service (GPS) satellite (e.g., page 16, lines 12-14, Figure 5). It should be noted that, in the claimed embodiment, both the first and second timing signals are received from
10 the same remote source, such a single GPS satellite (see, e.g., page 16, lines 8-11). As mentioned previously, embodiments of the present invention utilize the variances in arrival times of the timing signals as a source for an unpredictable random number, which is referred to as the “delay number.” Hence, as exemplified in claim 1, the method includes computing a delay number, which is a measure of the variation between arrival times of
15 the first and second timing signals at the receiver (e.g., page 25, lines 4-18). Environment information regarding the computer is then obtained. The environment information includes the aforementioned delay number and data concerning the operating environment of the computer (e.g., page 23, lines 6-12, page 25, lines 4-18, page 27, lines 5-9).

 The obtained environment information is then utilized to create an encryption key,
20 for example by hashing the environment information to create a new public/private key pair (see page 35 lines 5-17, Figure 12). Then, an electronic file is encrypted using the created encryption key (see page 33, lines 8-20). In this manner, the claimed invention generates self protecting electronic data files utilizing an environment profile that describes the operating environment of the client computer. Consequently, only a client
25 computer conforming to the operating environment as defined in the environment profile can access the data file (see page 33, lines 8-13).

 Independent claim 15 recites a method for protecting electronic files as recited with respect to claim 1, however, claim 15 further requires creating a decryption key based on a second operating environment profile to decrypt the electronic file. In particular,
30 independent claim 15 recites receiving first and second timing signals from a remote source using a receiver (e.g., page 16, lines 12-14, Figure 5) and computing a first delay number (e.g., page 25, lines 4-18) as described above with reference to claim 1. Claim 15

also recites storing an electronic file encrypted using an encryption key that is created using a first environment profile of the computer. As above, the environment profile includes the first delay number. (See page 33, lines 8-20, page 35 lines 5-17).

5 In addition, the embodiment of claim 15 requires creating a decryption key based on a second environment profile of the computer (see page 39, lines 7-12). Generally, this occurs after the file has been encrypted and stored. To access the file at a later time, a decryption key must be created as described next. Specifically, third and fourth timing signals are received from the same remote source as defined above using the receiver (e.g., page 39, lines 9-12, page 16, lines 12-14, Figure 5). The second environment profile
10 includes a second delay number computed, similar to above, utilizing the third and fourth timing signals from the remote source. A decryption key is then created based on the second environment profile of the computer, and the electronic file is decrypted using the decryption key (e.g., page 40 lines 3-9 and lines 16-17).

Claim 15 describes how the invention generates self protecting electronic data files
15 utilizing an environment profile that describes the operating environment of the client computer. Consequently, only a client computer conforming to the operating environment as defined in the environment profile can access the data file (see page 33, lines 8-13). To do this, the environment profile, which is based on the operating environment and a delay number, is processed to generate a new client public and private key pair, which is used for
20 file encryption (see page 40, lines 3-6). To access the file at a later date, a new key needs to be created as before. However, if there are any changes to the environment information of the computer, the created key will change, and thus be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the
25 encryption key which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the created key will not be able to decrypt the file, hence protecting the file from unauthorized access.

In a third embodiment, exemplified by independent claim 26, a method for protecting electronic files as described with reference to claim 1 is set forth with the
30 additional feature of authenticating a digital transaction using the delay number. Here, as above, first and second timing signals are received from a remote source using a receiver (e.g., page 16, lines 12-14, Figure 5). However, the embodiment of claim 26 further

authenticates a digital transaction using a delay number (see, e.g., page 30, lines 21-23, and page 31 lines 1-9), which as above, is a measure of the variation between arrival times of the first and second timing signals at the receiver (e.g., page 25, lines 4-18). Environment information regarding the computer is then obtained that includes the aforementioned delay number and data concerning the operating environment of the computer (e.g., page 23, lines 6-12, page 25, lines 4-18, page 27, lines 5-9). The obtained environment information is then utilized to create an encryption key, and an electronic file is encrypted using the created encryption key (see page 33, lines 8-20, page 35 lines 5-17).

10 VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1 - Whether claims 1-6, 15-22, 26, and 28-29 are patentable under 35 USC 102 over Fischer '617?

Issue 2 - Whether claims 7-9 and 23 are patentable under 35 USC 103 over Fischer in view of Overfield '577?

15 Issue 3 - Whether claims 10-14 and 24-25 are patentable under 35 USC 103 over Fischer in view of Schneck et al '498?

VII. ARGUMENTS

20 ***ISSUE 1 - WHETHER CLAIMS 1-6, 15-22, 26, AND 28-29 ARE PATENTABLE UNDER 35 USC 102 OVER FISCHER '617?***

For each ground of rejection which appellant contests herein which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

Claims 1-6

25 Independent claim 1 recites a method for digital authentication that requires, 1) receiving two timing signals from *the same remote source* using a receiver and 2) computing a value that is a measure of the *variation between arrival times of the two timing signals* at the receiver. This value is referred to as a "delay number" in the instant application.

Contrary to the present invention, the Fischer reference '617 teaches a method for providing location certificates wherein a position determination unit (PDU) 1 computes the unit's current location utilizing a conventional Loran and/or GPS apparatus. Columns 2-3, lines 65-3, of the '617 patent are relevant here and duplicated below for convenience of review:

The PDU 1 includes conventional position determining apparatus for receiving Loran and/or GPS signals and for computing its position. The current location or position may be continuously computed and maintained, or it may be computed only in response to a request.

As is well known, a conventional GPS apparatus utilizes signals from three or more GPS satellites to *triangulate* the current position of the apparatus. Similarly, a conventional Loran (Long Range Navigation) apparatus utilizes signals from three or more transmitter stations to triangulate the current position of the apparatus.

In other words, the PDU 1 of the Fischer reference utilizes a plurality of signals from different sources to triangulate its position. In fact, the method and apparatus disclosed in the Fischer reference generally cannot properly operate utilizing a single remote source because there would be no way to calculate its current location without utilizing three or more remote sources to triangulate its position.

The Examiner stated that "the first and second timing signals could still be broadly interpreted as being from multiple remote sources, each of which is itself 'a remote source', with the same analogous argument applying to the receiver." (see Final Office Action of January 17, 2006, page 18). Claim 1 recites: "receiving first and second timing signals from a remote source using a receiver." Clearly, claim 1 requires both the first and second timing signals to come from a *single* remote source. Although, as the Examiner stated, each of multiple remote sources is itself 'a remote source,' claim 1 still requires each remote source to provide *both* a first and second timing signal to the receiver.

Claim 1 further requires computing a value that is a measure of the variation between arrival times of the two timing signals, which are received from a single source as described above, at the receiver. This value is referred to as a "delay number" in the instant application. Although the Fischer reference may utilize timing signals from a plurality of remote sources to compute location, each timing signal is from a *different* satellite. Nowhere in the Fischer reference is there disclosed or reasonably suggested

measuring a variation between arrival times of two timing signals received from *a single source*, as required by claim 1. Although the Fischer reference mentions utilizing synchronized clocks in the LCU and beacons to combat spoofing (see Fischer '617, col. 4, lines 10-27), the Fischer reference discloses comparing the arrival time of a single timing signal verses an expected arrival time of the timing signal. This is not the same as measuring the *variance* between arrival times of *two timing signals from a single remote source*, as required by claim 1. Again, it should be borne in mind that both timing signals are received from the same remote source.

The Fischer reference also does not disclose nor reasonably suggest obtaining environment information regarding the computer, where the environment information includes the delay number, as required by independent claim 1. It should be borne in mind that the delay number is a measure of a variation between arrival times of the first and second timing signals, which as argued above, the Fischer reference does not disclose. The environment information is then utilized to create an encryption key.

Specifically, claim 1 requires “creating an encryption key based on the environment information; and encrypting an electronic file using the encryption key.” In this manner, claim 1 describes how the invention generates self protecting electronic data files utilizing an environment profile that describes the operating environment of the client computer. Consequently, only a client computer conforming to the operating environment as defined in the environment profile can access the data file (see page 33, lines 8-13). To do this, the environment information (i.e., environment profile) is appended to a passphrase and hashed to create a current key hash code. That is, the environment profile and the appended passphrase are processed to generate a new client public and private key pair, which is used for file encryption (see page 40, lines 3-6). To access the file at a later date, a new key needs to be created as before. However, if there are any changes to the environment information of the computer, the created key will change, and thus be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the encryption key which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the created key will not be able to decrypt the file, hence protecting the file from unauthorized access.

The Fischer reference does not disclose using computer environment information to create an encryption key. Quite to the contrary, the Fischer reference selects a predetermined encryption key to encrypt the location information provided by the PDU unit, but does not disclose *creating* an encryption key based on the environment information, as required by independent claim 1. Indeed, the Fischer reference does not disclose creating an encryption key at all, much less creating an encryption key based on characteristics of the computer's operating environment using a delay number as claimed.

Claims 2-6, each ultimately dependent from independent claim 1, are considered allowable by virtue of their dependencies. Claim 2 is further considered allowable on its own merits as it recites other features of the invention neither taught nor suggested by the Fischer reference. Claim 2 recites creating a decryption key based on environment information that can be utilized to decrypt the electronic file. The Fischer reference does not disclose creating any keys at all, much less decryption keys based on characteristics of the computer's operating environment using a delay number as claimed.

Claims 15-22

These claims generally recite a method for protecting electronic files as recited in claim 1, however, these claims further require creating a decryption key based on a second operating environment profile, which includes a delay number, to decrypt the electronic file.

In particular, independent claim 15 recites receiving first and second timing signals from a remote source using a receiver and computing a first delay number as described above with reference to claim 1. Claim 15 also recites storing an electronic file encrypted using an encryption key that is created using a first environment profile of the computer. As above, the environment profile includes the first delay number. Thus, for the reasons advanced with respect to claim 1, claim 15 is considered patentable over the art of record.

In addition, claim 15 recites creating a decryption key based on a second environment profile of the computer. The second environment profile includes a second delay number computed, as above, utilizing third and fourth timing signals from *the* remote source. It should be noted that the antecedent bases for "*the* remote source" recited in claim 15 is the term "*a* remote source" named earlier in the claim. As such, claim 15 requires all four timing signals to be received from the *same* remote source. As set forth

above, the Fischer reference does not disclose nor reasonably suggest measuring the variance in arrival times of two signals from a single remote source.

As mentioned above, the Fischer reference does not disclose using computer environment profile information to create an encryption key and a decryption key. Quite
5 to the contrary, the Fischer reference selects a predetermined encryption key to encrypt the location information provided by the PDU unit, but does not disclose *creating* an encryption key based on the environment information, as required by independent claim 1. As noted above, the Fischer reference does not disclose creating encryption or decryption keys at all, much less creating these keys based on characteristics of the computer's
10 operating environment using a delay number as claimed.

The Examiner's vague assertion that "col. 1, lines 5-col.4, line 27 (of the Fischer reference) whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to encrypted and clearly stored files via standard log-in/log-on) via the LCU based certificate aspect" (see Final Office action page 7) does not
15 address this aspect of the claimed invention. Similarly, the Examiners further statement that "the physical location aspect of the LCU is public key based (i.e., col. 3, lines 15-col. 4, line 10) because the certificate is public key based (the key certified by virtue of the certificate), and the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65))" (See *Id.*) also does not address this aspect of the
20 claim invention. That is, simply stating that the Fischer reference is public key based does not show anticipation. To anticipate the claimed invention, the Fischer reference must teach each aspect of the claimed invention. A vague idea of Fischer using public keys to encrypt data is not enough.

To anticipate the claimed invention, the Fischer reference must teach "*creating* a
25 decryption key *based* on a second environment profile of the computer" that itself is based on "the second delay number," as recited in claim 15, which the Fischer reference fails to do. As discussed previously, the Fischer reference does not disclose nor reasonably suggest calculating or storing first and second delay numbers as claimed. Further, the Fischer reference does not disclose nor reasonably suggest utilizing the delay numbers as
30 part of an environment profile. Moreover, the Fischer reference does not disclose nor reasonably suggest creating any encryption or decryption keys.

Claim 15 describes how the invention generates self protecting electronic data files utilizing an environment profile that describes the operating environment of the client computer. Consequently, only a client computer conforming to the operating environment as defined in the environment profile can access the data file (see page 33, lines 8-13). To do this, the environment profile, which is based on the operating environment and a delay number, is processed to generate a new client public and private key pair, which is used for file encryption (see page 40, lines 3-6). To access the file at a later date, a new key needs to be created as before. However, if there are any changes to the environment information of the computer, the created key will change, and thus be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the encryption key which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the created key will not be able to decrypt the file, hence protecting the file from unauthorized access.

There is simply no mention of such a limitation in the Fischer reference, and as mentioned above, it is unclear from the Examiner's vague Final Rejection how specifically the Examiner feels the Fischer reference teaches these claimed features. It would be very helpful to the appellant and consistent with proper examination practice if the Examiner would kindly specifically indicate structures within the Fischer reference which teach specific claimed features. Claims 16-22, each ultimately dependent from independent claim 15, are considered allowable by virtue of their dependencies.

Claims 26, 28-29

Claim 26 is considered allowable for the same reasons set forth above with respect to claims 1 and 15. In addition, claim 26 requires authenticating a digital transaction using the delay number. The Fischer reference does not disclose nor reasonably suggest using a delay number, which is a measure of a variation between arrival times of the first and second timing signals, to authenticate a digital transaction, as required by independent claim 26. Quite to the contrary, the Fischer reference merely encrypts its location data and transmits it to a user. Embodiments of the claimed invention utilize the variances in timing signals from a single remote source as a resource for an unpredictable random number, which is referred to as the "delay number," for use in authenticating a digital transaction. The location calculated in the PDU 1 of the Fischer reference is not random in

the sense that it will be the same as long as the PDU 1 remains stationary. Indeed, the stationary aspect of the location is what the Fischer reference utilizes for certification. That is, if the location is not where it should be, the certificate is invalid. Random locations simply will not work in the Fischer reference. Claims 28-29, each ultimately dependent from independent claim 26, are considered allowable by virtue of their dependencies.

ISSUE 2 - WHETHER CLAIMS 7-9 AND 23 ARE PATENTABLE UNDER 35 USC 103 OVER FISCHER IN VIEW OF OVERFIELD '577?

10 **Claims 7-9 and 23**

To establish a prima facie case of obviousness, the references when combined must teach or suggest all the claim limitations. The Examiner has not established a prima facie case of obviousness because the references when combined do not teach or suggest all of the claim limitations. A prima facie case of obviousness requires that the reference teachings “appear to have suggested the claimed subject matter.” *In re Rinehart*, 531 F.2d 1048, 189 USPQ 143, 147 (CCPA 1976). Here, as argued above, the art of record does not teach nor reasonably suggest all the claim limitations of independent claims 1 and 15, from which claims 7-9 and 23 ultimately depend, respectively. Therefore, claims 7-9 and 23 are considered allowable over the art of record for at least the same reasons set forth above with reference to independent claims 1 and 15.

ISSUE 3 - WHETHER CLAIMS 10-14 AND 24-25 ARE PATENTABLE UNDER 35 USC 103 OVER FISCHER IN VIEW OF SCHNECK ET AL '498?

Claims 10-14 and 24-25

To establish a prima facie case of obviousness, the references when combined must teach or suggest all the claim limitations. The Examiner has not established a prima facie case of obviousness because the references when combined do not teach or suggest all of the claim limitations. A prima facie case of obviousness requires that the reference teachings “appear to have suggested the claimed subject matter.” *In re Rinehart*, 531 F.2d 1048, 189 USPQ 143, 147 (CCPA 1976). Here, as argued above, the art of record does not teach nor reasonably suggest all the claim limitations of independent claims 1 and 15, from which claims 10-14 and 24-25 ultimately depend, respectively. Therefore, claims 10-

14 and 24-25 are considered allowable over the art of record for at least the same reasons set forth above with reference to independent claims 1 and 15.

Conclusion


5 For the extensive reasons advanced above, Appellant respectfully but forcefully contends that each claim is patentable. Therefore, reversal of all rejections is courteously solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby requested.

10

Respectfully Submitted,
PATENT VENTURE GROUP
A PROFESSIONAL LAW CORPORATION

15


Joe A. Brock II, Esq.
Reg. No. 46,021

20

PATENT VENTURE GROUP
A PROFESSIONAL LAW CORPORATION
10788 Civic Center Drive, Suite 215
25 Rancho Cucamonga, California 91730
909.758.5145



APPENDIX A

CLAIMS ON APPEAL

1. A method for protecting electronic files, comprising:

receiving first and second timing signals from a remote source using a receiver;

5 computing a delay number, the delay number being a measure of a variation
between arrival times of the first and second timing signals at the receiver;

obtaining environment information regarding a computer, the environment
information including the delay number and data concerning an operating environment
of the computer;

10 creating an encryption key based on the environment information; and

encrypting an electronic file using the encryption key.
2. A method as recited in claim 1, further comprising the operation of
creating a decryption key based on environment information, wherein the decryption
15 key can be utilized to decrypt the electronic file.
3. A method as recited in claim 2, wherein the encryption key and the
decryption key are public key infrastructure (PKI) based keys.
- 20 4. A method as recited in claim 1, wherein the environment information

includes location information of the computer.

5. A method as recited in claim 4, wherein the location information specifies a location of the computer within a predetermined range.

5

6. A method as recited in claim 5, wherein the location information is provided by global positioning satellite (GPS) data.

7. A method as recited in claim 1, wherein the environment information
10 includes drive information regarding a drive wherein the electronic file will be stored.

8. A method as recited in claim 7, wherein the drive information includes a drive identifier that identifies the particular drive wherein the electronic file will be stored.

15

9. A method as recited in claim 7, wherein the drive information includes an electronic address assignment of the particular drive wherein the electronic file will be stored.

20 10. A method as recited in claim 1, wherein the environment information

includes time information specifying access duration.

11. A method as recited in claim 10, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.

5

12. A method as recited in claim 11, wherein the electronic file cannot be decrypted at a time outside the time range.

13. A method as recited in claim 10, wherein the access duration is a date range indicating a range of dates when the electronic file can be accessed.

10

14. A method as recited in claim 13, wherein the electronic file cannot be decrypted at a date outside the date range.

15. A method for protecting electronic files, comprising:

15

receiving first and second timing signals from a remote source using a receiver;

computing a first delay number, the first delay number being a measure of a variation between arrival times of the first and second timing signals at the receiver;

storing an electronic file encrypted using an encryption key, wherein the

encryption key is created using a first environment profile of a computer, and wherein the environment profile includes the first delay number and data concerning an operating environment of the computer;

receiving third and fourth timing signals from the remote source using the
5 receiver;

computing a second delay number, the second delay number being a measure of a variation between arrival times of the third and fourth timing signals at the receiver;

creating a decryption key based on a second environment profile of the computer, the second environment profile being based on a current operating
10 environment of the computer and the second delay number; and

decrypting the electronic file using the decryption key.

16. A method as recited in claim 15, wherein the encryption key and the decryption key are further based on a passcode received from a user.

15

17. A method as recited in claim 16, further comprising the operation of appending the first environment profile to the passcode to generate the encryption key.

18. A method as recited in claim 17, further comprising the operation of
20 appending the current environment profile to the passcode to create the decryption key.

19. A method as recited in claim 18, wherein the decryption key cannot decrypt the electronic file when the current environment profile does not match the first environment profile.

5

20. A method as recited in claim 19, wherein a match occurs when the data in the current environment profile is within a predetermined range of the data in the first environment profile.

10 21. A method as recited in claim 15, wherein the environment profile includes location information specifying a location of the computer within a predetermined range.

22. A method as recited in claim 21, wherein the location information is
15 provided by global positioning satellite (GPS) data.

23. A method as recited in claim 15, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.

20 24. A method as recited in claim 15, wherein the environment information

includes time information specifying access duration, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.

25. A method as recited in claim 15, wherein the environment information
5 includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.

26. A method for protecting electronic files, comprising:

receiving first and second timing signals from a remote source using a receiver;

10 authenticating a digital transaction using a delay number, the delay number being a measure of a variation between arrival times of the first and second timing signals at the receiver;

obtaining environment information regarding a computer, the environment information including the delay number and data concerning an operating environment
15 of the computer;

creating an encryption key based on the environment information; and

encrypting an electronic file using the encryption key.

27. (canceled)

20

28. A method as recited in claim 26, wherein the delay in the timing signal is caused by free electrons in a line of sight between the remote source and a receiver.

29. A method as recited in claim 28, wherein the delay in the timing signal is
5 further caused by variations in atmospheric conditions.

APPENDIX B

EVIDENCE

- 5 1. **U.S. Patent No. 5,659,617 to Fischer;** Entered into record by Examiner in Office
Action dated 8/27/2004.
2. **Office Action dated 1/17/2006.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,572	10/30/2001	Roger R. Dube	GATEP002	4976

52785 7590 01/17/2006

PATENT VENTURE GROUP
10788 CIVIC CENTER DRIVE
SUITE 215
RANCHO CUCAMONGA, CA 91730

EXAMINER

BAUM, RONALD

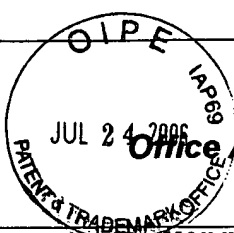
ART UNIT PAPER NUMBER

2136

DATE MAILED: 01/17/2006



Please find below and/or attached an Office communication concerning this application or proceeding.



Office Action Summary

Application No.

10/003,572

Applicant(s)

DUBE, ROGER R.

Examiner

Ronald Baum

Art Unit

2136

The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 October 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26, 28 and 29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26, 28, 29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 17 October 2005.
2. Claims 1- 26,28,29 are pending for examination.
3. Claims 1- 26,28,29 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6,15-22,26,28,29 are rejected under 35 U.S.C. 102(e) as being anticipated by Fischer, U.S. Patent 5,659,617.

5. As per claim 1; "A method for protecting electronic files, comprising:

receiving first and second timing signals from

a remote source using a receiver;

computing a delay number, the delay number being

a measure of a variation between

arrival times of the first and

second timing signals at the receiver; [col. 1,lines 5-col. 4,line 27,

whereas information regarding physical location via the LCU based

certificate aspect is GPS based; such that it is inherent that the GPS

functionality is derived from the fact that GPS determined location is a function of the differential delays processed from received timing signals (i.e., 'delay time period between') from (i.e., 'timing signals from a remote source') an associated plurality of GPS satellites.];

obtaining environment information regarding a computer,

the environment information including

the delay number and

data concerning an operating environment of the computer [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect];

creating an encryption key based on

the environment information [col. 1,lines 5-col. 4,line 27, whereas the physical location aspect of the LCU is public key based (i.e., col. 3,lines 15-col. 4,line 10) because the certificate is public key based (the key certified by virtue of the certificate). Further, the certificate created is inherently a function of the LCU and more specifically a function of the location (i.e., '...creating an encryption key ... environment information ...') of the LCU.]; and

encrypting an electronic file using

the encryption key [col. 1,lines 5-col. 4,line 27, whereas the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65).].”.

6. Claim 2 *additionally recites* the limitation that; “A method as recited in claim 1, further comprising

the operation of creating a decryption key based on
environment information,
wherein the decryption key can be utilized to
decrypt the electronic file.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

7. Claim 3 *additionally recites* the limitation that; “A method as recited in claim 2, wherein

the encryption key and
the decryption key
are
public key infrastructure (PKI) based keys.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65) which is certified to assure proper association of the

Art Unit: 2136

public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

8. Claim 4 ***additionally recites*** the limitation that; “A method as recited in claim 1, wherein the environment information includes
location information of the computer.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect.).

9. Claim 5 ***additionally recites*** the limitation that; “A method as recited in claim 4, wherein the location information specifies
a location of the computer within a predetermined range.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas environment information regarding physical location via the LCU based certificate aspect is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5, lines 9-col. 9, line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

10. Claim 6 ***additionally recites*** the limitation that; “A method as recited in claim 5, wherein the location information is provided by
global positioning satellite (GPS) data.”.

Art Unit: 2136

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas environment information regarding physical location via the LCU based certificate aspect is GPS based.).

11. As per claim 15; "A method for protecting electronic files, comprising:

receiving first and second timing signals from

a remote source using a receiver;

computing a delay number, the delay number being

a measure of a variation between

arrival times of the first and

second timing signals at the receiver; [col. 1, lines 5-col. 4, line 27,

whereas information regarding physical location via the LCU based

certificate aspect is GPS based; such that it is inherent that the GPS

functionality is derived from the fact that GPS determined location is a

function of the differential delays processed from received timing signals

(i.e., 'delay time period between') from (i.e., 'timing signal was

transmitted from a remote source') an associated plurality of GPS

satellites.];

storing an electronic file encrypted using an encryption key,

wherein the encryption key is created using a first environment profile of a

computer, and

wherein the environment profile includes the first delay number and data concerning an operating environment of the computer [col. 1, lines 5-col. 4, line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to encrypted and clearly stored files via standard log-in/log-on) via the LCU based certificate aspect. Further, the physical location aspect of the LCU is public key based (i.e., col. 3, lines 15-col. 4, line 10) because the certificate is public key based (the key certified by virtue of the certificate), and the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65).];

receiving third and fourth timing signals from

a remote source using a receiver;

computing a second delay number, the second delay number being

a measure of a variation between

arrival times of the third and

fourth timing signals at the receiver, [col. 1, lines 5-col. 4, line 27, whereas

information regarding physical location via the LCU based certificate aspect is GPS based; such that it is inherent that the GPS functionality is derived from the fact that GPS determined location is a function of the differential delays processed from received timing signals (i.e., 'delay time period between') from (i.e., 'timing signal was transmitted from a remote source') an associated plurality of GPS satellites.];

creating a decryption key based on a second environment profile of the computer,
the second environment profile being based on a current operating environment of the computer [col. 1, lines 5-col. 4, line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., during second operating environment of the computer data collection for the purpose of comparison of profile information for the explicit purpose of file access of to encrypted and clearly stored files via standard log-in/log-on) via the LCU based certificate aspect] and;

decrypting the electronic file using the decryption key [col. 1, lines 5-col. 4, line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality. Further, the certificate created is inherently a function of the LCU and more specifically a function of the location (i.e., ... creating a decryption key ... second environment profile ...') of the LCU.]”.

12. Claim 16 ***additionally recites*** the limitation that; “A method as recited in claim 15, wherein the encryption key and the decryption key are further based on a passcode received from a user.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65), and further layered access control derived from using said certificate, is associated with the use of

Art Unit: 2136

PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

13. Claim 17 *additionally recites* the limitation that; “A method as recited in claim 16, further comprising the operation of appending the first environment profile to the passcode to generate the encryption key.”.

The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

14. Claim 18 *additionally recites* the limitation that; “A method as recited in claim 17, further comprising the operation of appending the current environment profile to the passcode to create the decryption key.”.

The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5). Further, the certificate created is inherently a function of the LCU and more specifically a function of the location (i.e., ‘... create the decryption key ...’) of the LCU.).

15. Claim 19 *additionally recites* the limitation that; “A method as recited in claim 18, wherein the decryption key cannot decrypt the electronic file when the current environment profile does not match the first environment profile.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3, lines 63-col. 4, line 10, col. 10, lines 45-col. 11, line 5).).

16. Claim 20 *additionally recites* the limitation that; “A method as recited in claim 19, wherein a match occurs when the data in the current environment profile is within a predetermined range of the data in the first environment profile.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2, lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3, lines 63-col. 4, line 10, col. 10, lines 45-col. 11, line 5). Further, whereas the aspect of the environment information regarding physical location via the LCU based certificate is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5, lines 9-col. 9, line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

Art Unit: 2136

17. Claim 21 *additionally recites* the limitation that; “A method as recited in claim 15, wherein the environment profile includes location information specifying a location of the computer within a predetermined range.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas environment information regarding physical location via the LCU based certificate aspect is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5, lines 9-col. 9, line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

18. Claim 22 *additionally recites* the limitation that; “A method as recited in claim 21, wherein the location information is provided by global positioning satellite (GPS) data.”.

The teachings of Fischer suggest such limitations (col. 1, lines 5-col. 4, line 27, whereas environment information regarding physical location via the LCU based certificate aspect is GPS based.).

19. As per claim 26; “A method for protecting electronic files comprising;

receiving first and second timing signals from

a remote source using a receiver;

authenticating a digital transaction using a delay number the delay number being

a measure of a variation between

arrival times of the first and

second timing signals at the receiver; [col. 1, lines 5-col. 4, line 27, whereas information regarding physical location via the LCU based certificate aspect is GPS based; such that it is inherent that the GPS functionality is derived from the fact that GPS determined location is a function of the differential delays processed from received timing signals (i.e., 'delay time period between') from (i.e., 'timing signals from a remote source') an associated plurality of GPS satellites.];

obtaining environment information regarding a computer, the environment information including

the delay number and

data concerning an operating environment of the computer [col. 1, lines 5-col. 4, line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect];

creating an encryption key based on the environment information [col. 1, lines 5-col. 4, line 27, whereas physical location aspect of the LCU is public key based (i.e., col. 3, lines 15-col. 4, line 10) because the certificate is public key based (the key certified by virtue of the certificate). Further, the certificate created is inherently a function of the LCU and more specifically a function of the location (i.e., '...creating an encryption key ... environment information ...') of the LCU.]; and

Art Unit: 2136

encrypting an electronic file using the encryption key [col. 1,lines 5-col. 4,line 27, whereas the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65).].”.

20. Claim 28 *additionally recites* the limitation that; “A method as recited in claim 26, wherein the delay in the timing signal is caused by free electrons in a line of sight between the remote source and a receiver.”.

The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computers physical location as a function of GPS (i.e., col. 2,lines 3-19, col. 4,lines 27-col. 5,line 22) via the LCU based certificate clearly uses remote source (GPS satellite transmission) to LCU (receiving said transmission) and the delay in the timing signal is inherently a timing aspect caused by free electrons in a line of sight between the remote source and a receiver.).

21. Claim 29 *additionally recites* the limitation that; “A method as recited in claim 28, wherein the delay in the timing signal is further caused by variations in atmospheric conditions.”.

The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas for GPS using remote source (GPS satellite transmission) to LCU (receiving said transmission) delay in the timing signal is inherently a timing aspect further caused by the variations in atmospheric conditions.).

Claim Rejections - 35 USC § 103

Art Unit: 2136

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

22. Claims 7-9,23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer, U.S. Patent 5,659,617 as applied to claims 1,15,26 respectively, above, and further in view of Overfield, U.S. Patent 5,598,577.

Claim 7 *additionally recites* the limitation that; "A method as recited in claim 1, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.";

Claim 8 *additionally recites* the limitation that; "A method as recited in claim 7, wherein the drive information includes a drive identifier that identifies the particular drive wherein the electronic file will be stored.";

Claim 9 *additionally recites* the limitation that; "A method as recited in claim 7, wherein the drive information includes an electronic address assignment of the particular drive wherein the electronic file will be stored.";

Claim 23 *additionally recites* the limitation that; "A method as recited in claim 15, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored."

The teachings of Fischer suggest base claims ("A method for protecting electronic files, comprising: obtaining environment information regarding a computer, the environment information including data concerning an operating, environment of the computer...")

limitations (Abstract, col. 1, lines 5-col. 4, line 27, col. 5, lines 9-col. 9, line 31) *without explicitly teaching* of the use of “environment information includes drive information [including ‘electronic address assignment’] regarding a drive wherein the electronic file will be stored”.

Overfield teaches of using; “[system software] queries a disk drive to determine its model. The system software checks the corresponding response string with reference to a table of recognized model strings (in encrypted format). If the drive’s response string is recognized in this table, then the drive parameters can be set appropriately. [Abstract, col. 1, lines 32-col. 4, line 45]” Such that “the corresponding response string” clearly corresponds to drive information (including “electronic address assignment”).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Overfield disk drive query/response parameter authentication and authorization invention, to the Fischer method/system protecting electronic files via obtaining environment information (location certificate based) regarding a computer.

Such motivation to combine would clearly encompass the need to allow for qualitatively superior authentication scenario to improve security in a disk file configured computer system, whereas the authentication and authorization for file access (i.e., disk drive specific via drive configuration) clearly is a function of said disk drive query/response parameters. (i.e., col. 9, line 62-col. 10, line 54).

23. Claims 10-14, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer, U.S. Patent 5,659,617 as applied to claims 1, 15, 26 respectively, above, and further in view of Schneck et al, U.S. Patent 5,933,498.

Art Unit: 2136

Claim 10 *additionally recites* the limitation that; “A method as recited in claim 1, wherein the environment information includes time information specifying access duration.”;

Claim 11 *additionally recites* the limitation that; “A method as recited in claim 10, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.”;

Claim 12 *additionally recites* the limitation that; “A method as recited in claim 11, wherein the electronic file cannot be decrypted at a time outside the time range.”;

Claim 13 *additionally recites* the limitation that; “A method as recited in claim 10, wherein the access duration is a date range indicating a range of dates when the electronic file can be accessed.”;

Claim 14 *additionally recites* the limitation that; “A method as recited in claim 13, wherein the electronic file cannot be decrypted at a date outside the date range.”;

Claim 24 *additionally recites* the limitation that; “A method as recited it claim 15, vvherein the environment information includes time information specifying access duration, wherein the access duration is a time range indicating a tine period when the electronic file can be accessed.”;

Claim 25 *additionally recites* the limitation that; “A method as recited it claim 15, wherein the environment information includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.”.

The teachings of Fischer suggest base claims (“A method for protecting electronic files, comprising: obtaining environment information regarding a computer, the environment

Art Unit: 2136

information including data concerning an operating environment of the computer...”)

limitations (Abstract, col. 1, lines 5-col. 4, line 27, col. 5, lines 9-col. 9, line 31) *without explicitly teaching* of the use of “time [and date] range indicating a time period [and date period] when the electronic file can [and can’t] be accessed [decrypted]”.

Schneck et al teaches of using; “A method and device are provided for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules...[Abstract], and further; “The invention can restrict the qualities or quantities of access to data in any manner that can be calculated or enumerated. A non-exhaustive, representative set of examples is given below...” [col. 25, lines 6-col. 27, line 27]” such that “the non-exhaustive, representative set of examples is given below...[list]” clearly corresponds to “time [and date] range indicating a time period [and date period] when the electronic file can [and can’t] be accessed [decrypted]” via the specific policy creation as used for the said encryption/decryption and access control functionality.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Schneck et al policy based access control

Art Unit: 2136

invention, to the Fischer method/system protecting electronic files via obtaining environment information (location certificate based) regarding a computer.

Such motivation to combine would clearly encompass the need to allow for qualitatively superior authentication scenario to improve security in a disk file configured computer system, whereas the authentication and authorization for file access (i.e., disk drive specific via drive configuration) clearly is a function of said disk drive policy access time, date, etc., criteria. (i.e., Abstract, col. 6,line 49-col. 8,line 47, col. 25,lines 6-col. 27,line 27).

Response to Amendment

24. As per applicant's argument concerning the lack of teaching by Fischer of the same "single" remote source and receiver, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The amended claim language is still too broad in that as phrased, the first and second timing signals could still be broadly interpreted as being from multiple remote sources, each of which is itself "a remote source", with the same analogous argument applying to the receiver. Therefore, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that the rejection support reference collectively encompass the said claim limitations in their entirety.

25. As per applicant's argument concerning the lack of teaching by Fischer of the "... creating an encryption key ..." limitations, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The rejection is described above

Art Unit: 2136

in the claim 1, et seq., argument dealing with “the physical location aspect of the LCU is public key based ...”. Therefore, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that the rejection support reference collectively encompass the said claim limitations in their entirety.

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2136

Conclusion

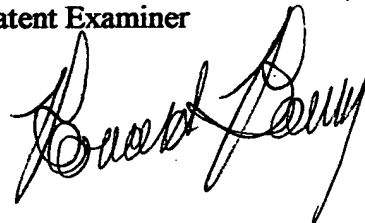
27. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100



APPENDIX C
RELATED PROCEEDINGS

None